

DHCP Snooping



DAVID BOMBAL
EDUCATE.MOTIVATE

SEARCHING.....

DHCP Snooping

- Want to watch a YouTube video?
 - <https://youtu.be/S6KI6VsvDuU>



DHCP Snooping

- DHCP Snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers.



DHCP Snooping

- Performs the following activities:
 - Validates DHCP messages received from untrusted sources and filters out invalid messages.
 - Rate-limits DHCP traffic from trusted and untrusted sources.



DHCP Snooping

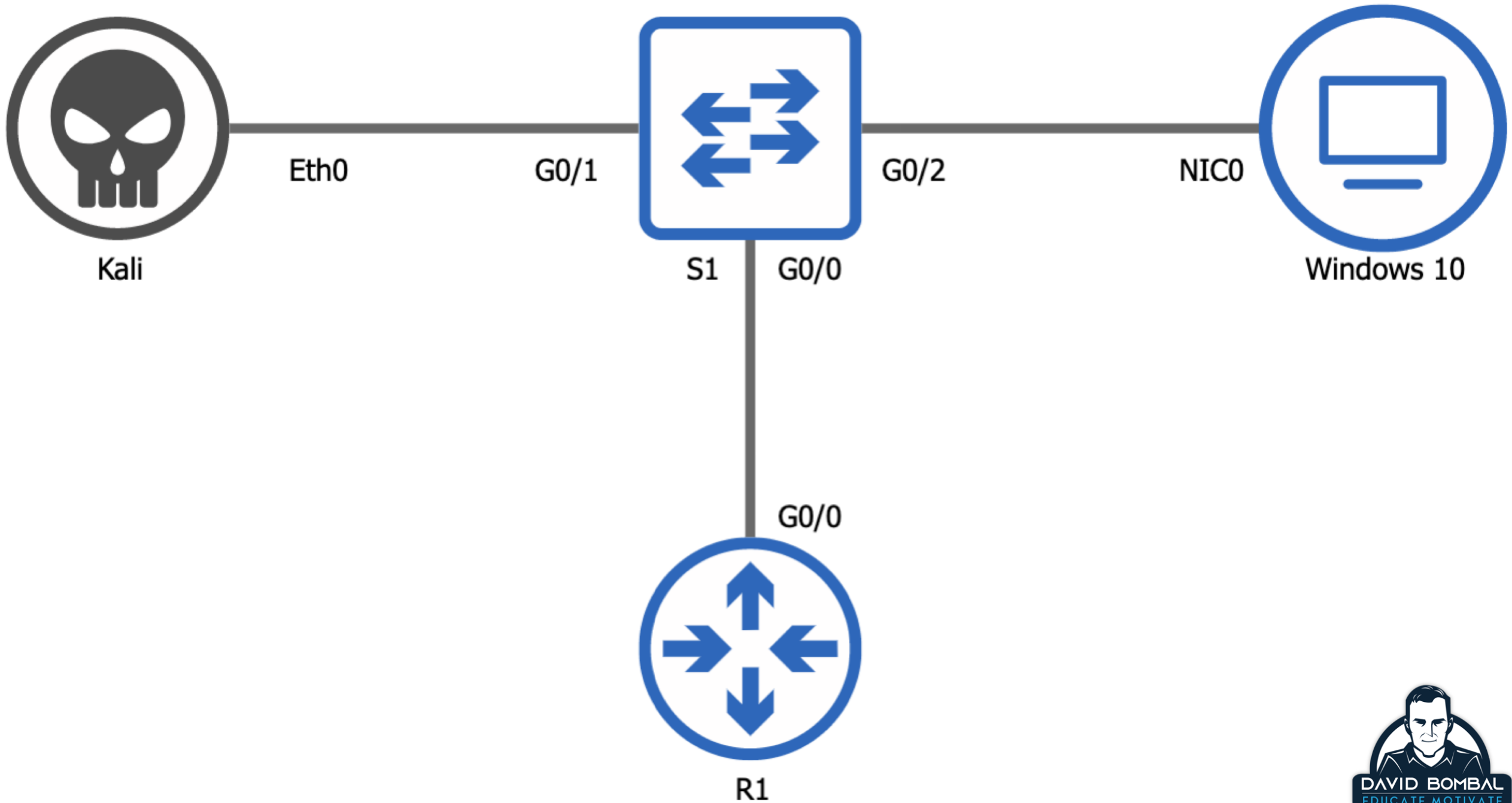
- Performs the following activities:
 - Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.



DHCP Snooping

- Performs the following activities:
 - Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.





DHCP Configuration

- Configuration examples per network diagram
 - Substitute VLAN 1 with your VLAN
 - Substitute g0/0 and g0/1 with the interfaces you use



Configuration Part 1

- Enable DHCP snooping:
 - `conf t`
 - `ip dhcp snooping`
 - `ip dhcp snooping vlan 1`
 - `no ip dhcp snooping information option`
 - `exit`
 - `show ip dhcp snooping`



Configuration Part 2

- Specify trusted ports:
 - `conf t`
 - `int G0/0`
 - `ip dhcp snooping trust`



Configuration Part 3

- Optional: Rate limit untrusted ports (packets per second):
 - `int G0/1`
 - `ip dhcp snooping limit rate 10`
 - `end`



Configuration Part 4

- Optional: Auto-recover err-disabled ports after 30 seconds:
 - `conf t`
 - `errdisable recovery cause dhcp-rate-limit`
 - `errdisable recovery interval 30`
 - `end`



Verification

- Verify that it is working:
 - `show ip dhcp snooping`
 - `debug ip dhcp snooping events`
 - `debug ip dhcp snooping packets`



DHCP Snooping

- Go here for more:
 - <http://bit.ly/ciscodhcp>
 - <http://bit.ly/dhcpsnoop>
 - <http://www.davidbombal.com>



DHCP Snooping



DAVID BOMBAL
EDUCATE.MOTIVATE